Case Studies: Mapping Products to Compliance

Vik Phatak
CEO
NSS Labs
Vik Phatak, CEO, NSS Labs

• Expert on vulnerability management and threat protection.
• Served as CTO for Trustwave (ATW), the world’s largest PCI assessor.
• Founded Lucid Security and developed one of the leading IPS appliances for enterprises.
• Global Manager of Enterprise Internet and Security Services at Teleflex, a publicly-traded global manufacturing company.
• Co-founder of Intermedia Sciences Group, Inc., a security consulting firm.

NSS Labs

• A leading independent security product testing and certification lab.
• Performs product feature validation testing for PCI DSS requirements
• Tests & certifies firewalls, Network & Host IPS, UTM, Wireless, PKI/Encryption, DLP, Vulnerability Scanner, more.
• Largest security & performance testing lab in the world.
Agenda

- Approaches Review – Mapping compliance to technology choice
- Case studies
  - Retail organization - PCI
  - Healthcare - HIPAA + PCI
  - Manufacturing - SOX
Approaches Review

- Aim for security and achieve compliance (gap analysis, multiple compliance reqs?)
- Know where your data is
- Determine protection requirements
- Limit scope (data flows, retention)
- Products, People or Processes
- Seek answers from vendors
Selecting The Right Products

Information Security Products are tools

- **Different products solve different problems**
  - Products fulfill specific purposes – You don’t expect your screwdriver to saw wood
  - Multi-function tools (i.e. Swiss army knife) do lots of things, but are not usually best at solving a specific problem
  - It is okay to have a favorite tool... just don’t expect it to be the only tool you will need
Selecting The Right Products

No product can MAKE you compliant...
...but the wrong products can impede your compliance efforts
Like the gist, hate the text. what concretely are we saying.

be able to DEFEND your choices?

Rick, 3/10/2008
Case Study – PCI DSS
PCI Compliance

• Retail Organization
  • Privately Held
    • 200 storefronts
    • 3 regional centers
    • 1 Corporate HQ
  • Technologies Required:
    • Firewall
    • IDS/IPS
    • AV
    • Encryption (data-in-motion)
    • Encryption (data-at-rest)
    • Identity Management
    • Log Management
Selecting The Right Products

- **Firewalls**
  - Separate Inside (trusted) from outside (un-trusted)
  - Traditionally Routing between Internal, External & DMZ networks
  - Used to limit Access to/from a network or systems on the network = Access Control
  - Operate at lower layers (IP, TCP, UDP, etc.)
  - Good at enforcing access. Not good at catching attacks.
  - Low maintenance & upkeep
  - Low granularity of control (control of protocols, not content)
Selecting The Right Products

- **What firewall requirements are we faced with?**
  - PCI DSS v1.1 Requirement #1 = Install & Maintain a firewall to protect cardholder data

- **Do they all “Segment”?**
  - Some firewalls only segment Internal from External despite multiple NICs, while others allow you to create logically separate segments (one per NIC).
  - Per-domain administration?
  - How are you planning on using the firewall?

- **Does the firewall encrypt all non-console administrative access?**

- **Does the firewall log all changes and provide a robust audit trail?**
Selecting The Right Products

**IDS/IPS**

- “Deep Inspection” = look into the payload of the traffic
- High Maintenance & Upkeep
- Good at catching known attacks (exploits) against systems with vulnerabilities
- Different brands/manufacturers have different strengths
  - Client Protection (Web Browsers, E-Mail Clients, etc.)
  - Server Protection (Web Servers, E-Mail Servers, etc.)
  - Internal Applications (File & Print, DB, etc.)
  - Application Vendors (Microsoft, Sun, Open Source)
  - Protocols – HTTP, HTTPS, SMTP, IMAP, Exchange, LDAP, DNS, RPC, NetBios, etc.
- Some Manufacturers: **BlueLane, Cisco, IBM/ISS, Juniper, McAfee, SecureComputing, Sourcefire, TippingPoint, Third Brigade, TrustWave**
PCI Compliance

- **Large Financial Institution & IDS/IPS**
  - PCI DSS v1.1 – Requirement 11.4:
    “Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.”
  - Claimed Firewall with “deep inspection” fulfilled IDS/IPS requirement because product vendor told them it would...
  - It was determined that the firewall with “deep inspection” did not meet compliance requirements because it did not adequately protect the systems in question (E-Commerce Servers)

11.1: Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.
PCI Compliance

Lesson Learned?
It is about a product’s ability to perform the necessary functions based upon how/where it is being used.

“Appropriate Usage”

The same firewall with deep inspection may have been appropriate to protect a retail storefront IF it was good at protecting against client attacks (IE, Firefox, Adobe, etc.)
Selecting The Right Products

- **IDS/IPS**
  - Host IPS
    - Strength is in stopping complex attacks that may get past other security
    - System Resource Intensive
    - Cannot stop attacks that compromise OS at a lower layer/before HIPS (i.e. NIC Drivers)
  - Network IPS
    - Good at stopping worms and fast moving attacks
    - Good at protecting against known vulnerabilities
    - Not good at stopping attacks against custom (web) apps
Selecting The Right Products

Common Protection Requirements

<table>
<thead>
<tr>
<th>ATTACKER INITIATED</th>
<th>CLIENT/TARGET INITIATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>RETAIL STOREFRONT</td>
<td>✓</td>
</tr>
<tr>
<td>CORPORATE PERIMETER</td>
<td>✓</td>
</tr>
<tr>
<td>E-COMMERCE DATACENTER</td>
<td>✓</td>
</tr>
<tr>
<td>INTERNAL DATACENTER</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INDUSTRY COMPARETTIVE RANKING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit Type</td>
</tr>
<tr>
<td>NIST EUK Average</td>
</tr>
<tr>
<td>Client Product</td>
</tr>
<tr>
<td>Data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PROTECTED ENVIRONMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Model</td>
</tr>
<tr>
<td>Client</td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Applications</td>
</tr>
<tr>
<td>Data Store</td>
</tr>
<tr>
<td>Retail Storefront</td>
</tr>
<tr>
<td>Corporate Perimeter</td>
</tr>
<tr>
<td>E-Commerce Datacenter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TARGETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTACKER INITIATED</td>
</tr>
<tr>
<td>RETAIL STOREFRONT</td>
</tr>
<tr>
<td>CORPORATE PERIMETER</td>
</tr>
<tr>
<td>E-COMMERCE DATACENTER</td>
</tr>
<tr>
<td>INTERNAL DATACENTER</td>
</tr>
</tbody>
</table>
Selecting The Right Products

- **UTM**
  - Multi-Function Device: FW + VPN + IPS + WF + AV
  - Evolved out of Firewalls – firewall usually strong
  - Decisions were made about what to emphasize – no product can be all things
    - Perimeter Devices - often cannot protect applications in the Core
    - Good at preventing people from bypassing Gateway AV (HTTP AV)
  - Different brands/manufacturers have different strengths
    - Client Protection (Web Browsers, E-Mail Clients, etc.)
    - Server Protection (Web Servers, E-Mail Servers, etc.)
    - Application Vendors (Microsoft, Sun, Open Source)
    - Protocols – HTTP, HTTPS, SMTP, IMAP, Exchange, DNS, RPC, etc.
  - Some Manufacturers: Cisco, Fortinet, IBM/ISS, Juniper, SecureComputing, 3Com/TippingPoint
Remote Office / Branch Office / Retail Storefront

No DMZ or servers facing the Internet

Internet

UTM Device

Internal Network

Internal User Browsing Internet

Small Request
Large Website Download
E-Commerce Datacenter

No client traffic initiated from DMZ – All traffic initiated from outside of the network

Internet

UTM Device

E-Commerce DMZ

Legitimate customers browse e-commerce website, send/receive email, etc.

Attackers initiate exploits against Internet facing servers/services

Does traffic contain attack against Apache/Tomcat Web Server?!
Typical Traffic Flow
Where is UTM Appropriate?

- PCI says nothing specifically about UTMs
- However, PCI does mention firewall, IDS/IPS, AV, & Encryption of data-in-motion (VPN)
- UTMs are not generally not “best of breed”
- Must examine the threat & risk dynamics:
  - UTMs good at protecting Internet Services
    - Retail Storefront (client protection)
    - Corporate Perimeter (both client & server)
    - SIMPLE E-Commerce sites
  - UTMs NOT good at protecting INTERNAL services (SQL, NetBios, etc.)
“Web-facing” Application Security

- **6.5 Secure coding**
  - OWASP Top 10 is a great start but... more than 10 significant vulnerability types in web apps
  - Other resources & tools

- **6.6 Code review or WAF**
  - Mandatory as of June 30, 2008
## Application Security Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Scanner (ext)</strong></td>
<td>• Systems&lt;br&gt;• Services</td>
</tr>
<tr>
<td><strong>Web App Firewall</strong></td>
<td>• Protects Applications, databases&lt;br&gt;• OWASP Top 10&lt;br&gt;• Usually in DMZ</td>
</tr>
<tr>
<td><strong>Web App Vulnerability Scanner</strong></td>
<td>• Scans Web Applications externally for flaws&lt;br&gt;• Highly specific</td>
</tr>
<tr>
<td><strong>Application Code Scanner</strong></td>
<td>• Programmatic analysis of source/binary code. Used to speed up a code review.</td>
</tr>
</tbody>
</table>
| **Code Review**                           | • Manual process of reading source code. Code Scanner used to make process more efficient.<br>• DSS 6.6 – best practice until June 30, 2008
Vulnerability Assessment (Scanner)

- Look for network and “common” application vulnerabilities – IIS, Apache, etc.
- Usually look for circumstantial evidence
  - Don’t run actual exploits – nobody wants their systems to be crashed or compromised
- Used as an information gathering tool
- Not conclusive, but are a good measuring tool nonetheless
- Some Manufacturers: IBM/ISS, N-Circle, Qualys, Saint, Tenable (Nessus)
Web App Vulnerability Scanner

- **Look for flaws in Web Applications**
  - Look deeper and more thoroughly than traditional Vulnerability Scanners
  - Detect unique flaws within Web Applications (i.e. SQL Injection, Form Validation errors, etc.)

- **Used as an information gathering tool**

- **Can be high maintenance - Some products are prone to false positives**

- **Will be required by June 30, 2008**

- **Some Manufactures: Appscan, Cenzic, NT Objectives, SPI Dynamics (HP), Watchfire (IBM), Whitehat**
Web App Firewall

- Compensating Control for PCI DSS 6.6 (vs. code review). June 30, 2008
- Enforce “positive” rules for Web Applications
  - Firewall for Layer-7
  - Look deeper than traditional Firewalls
  - Prevent flaws within Web Applications from being exploited (i.e. SQL Injection, Form Validation errors, etc.)
- Unforgiving: Only content you define as acceptable is allowed
- Some Manufactures: Barracuda, Breach, Citrix, F5, Fortify, eEye, Imperva, Mod Security, Sanctum
App Code Scanner (Static analysis)

- Examine the source code of Applications
  - Some can even examine binaries (Veracode)
  - Look for coding flaws
- Used as an information gathering tool
- Can be high maintenance
- Some Manufactures: Appscan, Cenzic, NT Objectives, SPI Dynamics (HP), Watchfire (IBM), Whitehat
- Not required by any Compliance regime, but it’s inefficient to perform a code review and not use an App Code Scanner
Anti-Malware (Anti-Virus)

- **Host**
  - Strength is in stopping complex attacks that may get past other security
  - Can be System Resource Intensive
  - Cannot stop attacks that compromise OS at a lower layer/before AM/AV (i.e. NIC Drivers)
  - Varying effectiveness (Strengths/Weaknesses) by product

- **Network/Gateway**
  - Email is not time-sensitive
  - May be bypassed by someone using webmail
  - Centralized – good at seeing patterns & being proactive on a macro level
Case Study - HIPAA + PCI
HIPAA + PCI Compliance

- Healthcare Organization
  - Privately Held
    - 4 Hospitals
    - 30 medical centers (doctor’s offices)
    - 1 Corporate HQ
  - Technologies Required:
    - Firewall
    - IDS/IPS
    - AV
    - Encryption (data-in-motion)
    - Encryption (data-at-rest)
    - Data Leak Prevention (DLP)
HIPAA + PCI Compliance

- **Data Leak Prevention (DLP)**
  - Requires a lot of ‘care & feeding’ to minimize false negatives & false positives
  - Good at stopping “Gilligan” but not “the Professor
  - Content:
    - Simple regex?
    - Context aware?
    - Partial fragment recognition?
  - Host: Good granular control, but resource intensive
  - Network: Good for specific data (Credit Card & Social Security numbers)
HIPAA + PCI Compliance

- **Encryption – data-in-motion**
  - Network-level tunneling (L2 and L3)
    - IPSec, some proprietary
  - Application-protocol-level tunneling
    - SSL VPN
  - Application-native crypto
  - Key management challenges – how does solution do provisioning, revocation?
    - Especially if multiple technologies in use
  - How does the solution deploy, protect and store key material / certificates? Concentration of risk ➔ audit risk
  - How is access control / key deployment auditable?
  - Impact on network latency and throughput?

HIPAA + PCI Compliance
HIPAA + PCI Compliance

- **Encryption – data-at-rest**
  - Full-disk encryption (hardware-level, driver-level)
  - File-level encryption (OS or third-party)
  - Application-native crypto – database, file
  - Key management challenges – provisioning, revocation
  - Key management challenges – how does solution do provisioning, revocation?
    - Especially if multiple technologies in use
  - How does the solution deploy, protect and store key material / certificates? Concentration of risk ➔ audit risk
  - How is access control / key deployment auditable?
  - Impact on I/O latency and throughput
    - Especially in the context of bulk storage – backup tapes
HIPAA + PCI Compliance

- **Encryption deployment example**
  - Healthcare provider implemented DBMS-level encryption
  - Disqualified as a mitigating control due to use of hard-coded keys
  - Key management is the hard part!
Case Study - SOX
SOX Compliance

- Mid-Sized Telecommunications Provider
  - Publicly Held
    - 15 corporate offices, 400+ POPs, 1000+ retail stores
    - 8000 employees
  - Technologies Required:
    - Firewall
    - IDS/IPS
    - AV
    - Encryption (data-in-motion)
    - Encryption (data-at-rest)
    - Identity Management
    - Log Management / SIM / SEM
SOX Compliance

- **Log Management / SIM / SEM**
  - SOX 404(a) requirement: “formal program” to retain, consolidate, and review log activity for all in-scope systems and devices including monitoring of change requests and authorization, user account authorizations and application and system access controls
  - What is breadth of device support (software, network, security?) – evaluate relative to unique environment
  - Data acquisition speed?
  - Agentless vs. agent-based?
  - Log storage – local, central, hierarchical/cached?
  - Speed of raw data retrieval?
  - Flexibility of Reporting (canned, custom), and speed of reporting
  - Correlation based on rates/counts/vulns/assets → quality of alerting
  - Actionability of alerting - reduction of false positives
  - Summarization (alert collapsing) – reduction of noise
SOX Compliance

- **Log Management / SIM / SEM**
  - SOX pre-audit situation
    - Log retention and aggregation in place
      - Homebrew solution based on EventLog and Syslog collection
    - Pre-audit testing found adequate control of log content to be lacking – no formal process for alerting/review based on real-time or retained log data
SOX Compliance

**Identity Management**

- SOX 404(a) requirement: “adequate internal controls” with respect to user access and privileges
- What is breadth of available Integration Points? (OS/software/network)
  - Authentication?
  - Granular, app-level authorization?
- User Provisioning – local/central/hierarchical/delegable?
- Role-based Management?
- Entitlement Management capabilities - relative to unique application footprint
- Identity Audit (IdA) capabilities
  - Access controls, authorization / privileges
  - Positive *and negative* reporting relative to HR systems
SOX Compliance

- **Identity Management**
  - Pre-audit situation
  - IdM in place
    - Major vendor solution
  - Pre-audit testing found adequate control of access rights to be lacking
    - No implementation of negative reporting relative to SAP/HR systems: inability to positively confirm that specific users did *not* have access to certain systems
Summary

- Map compliance requirements into security objectives, and RFPs
- Ensure people & processes can support effective use of products
- Track users & data. Segment to limit scope.
- Determine detailed protection requirements to show justification & set expectations
- If you can’t get answers from vendors it may be a fad